

**UNITED STATES OF AMERICA  
BEFORE THE FEDERAL TRADE COMMISSION**

**COMMISSIONERS:**      **Lina M. Khan, Chair**  
                                 **Rebecca Kelly Slaughter**  
                                 **Alvaro M. Bedoya**  
                                 **Melissa Holyoak**  
                                 **Andrew Ferguson**

**In the Matter of**  
  
**MARRIOTT INTERNATIONAL, INC.,**  
                 **a corporation**  
  
**and**  
  
**STARWOOD HOTELS & RESORTS**  
**WORLDWIDE, LLC,**  
                 **a limited liability company.**

**DOCKET NO.**

**COMPLAINT**

The Federal Trade Commission (“Commission”), having reason to believe that Marriott International, Inc., a corporation, and Starwood Hotels & Resorts Worldwide, LLC, a limited liability company (collectively, “Respondents”), have violated the provisions of the Federal Trade Commission Act, 15 U.S.C. § 45, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Marriott International, Inc. (“Marriott”) is a Delaware corporation with its principal office or place of business at 7750 Wisconsin Ave., Bethesda, Maryland 20814.

2. Respondent Starwood Hotels & Resorts Worldwide, LLC (“Starwood”) is a Maryland limited liability company with its principal office or place of business at 10000  
Maryland limited liability company with its principal office or place of business at 10000  
Maryland limited liability company with its principal office or place of business at 10000



### **Second Breach (Starwood)**

11. Despite having responsibility for Starwood's information security practices and network following the acquisition, Marriott failed to identify an ongoing breach within the Starwood network (hereinafter, the "Second Breach"). In fact, Marriott did not detect the Second Breach until September 7, 2018, nearly two years after the legal close of Marriott's acquisition of Starwood.

12. Forensic examiners determined that, on or about July 28, 2014, malicious actors compromised Starwood's external-facing webserver, installing malware on its network. This malware allowed the intruders to perform network reconnaissance activities, harvest highly privileged Starwood administrative and user credentials, and use those credentials to move throughout the Starwood's internal network for a four-year period, when Marriott's system finally detected an attempt to export consumer data from the guest reservation database on September 7, 2018.

13. Even after discovery of the breach, on September 10, 2018, the intruders exported additional guest information from Starwood's systems.

14. During this over four-year period, from July 2014 to September 2018—including the two years following Marriott's acquisition of Starwood and its integration of certain Starwood systems—the intruders went undetected, installing key loggers, memory-scraping malware, and Remote Access Trojans in over 480 systems across 58 locations within the Starwood environment. Those locations included a combination of corporate, data center, customer contact center, and hotel property locations.

15. Following the Second Breach, Respondents' forensic examiner assessed Starwood's systems and identified similar failures that resulted in the First Breach, including inadequate firewall controls, unencrypted payment card information stored outside of the secure cardholder data environment, lack of multifactor authentication, and inadequate monitoring and logging practices.

16. Due to the Second Breach, the personal information of 339 million consumer records globally was compromised, including more than 5.25 million unencrypted passport numbers. Additional compromised information included names, gender, dates of birth, payment card numbers, addresses, email addresses, telephone numbers, usernames, Starwood loyalty numbers, partner loyalty program numbers, and hotel stays and other travel information, such as location of hotel stays, duration of stays, number of children and guests, and flight information.

### **Third Breach (Marriott)**

17. The information security failures detailed in this Complaint are not limited to Starwood's computer networks, systems, and databases, nor are they limited to the First and Second Breaches that began during Starwood's control and operation of its information security program.



hotels, as well as Starwood-branded hotels.

26.

- g. Failed to apply adequate multifactor authentication to protect sensitive information. For example, Starwood failed to comply with contractual obligations and internal policies requiring multifactor authentication for remote access to sensitive environments, including environments containing payment card data.

### **Consumer Injury**

28. As a direct result of the failures described in Paragraph 27 above, between 2014 and 2020, malicious actors were able to gain unauthorized access to Respondents' networks in at least three separate breaches as described above. In the First Breach and Second Breach, the malicious actors used similar techniques, such as exploiting unpatched security vulnerabilities, remote access failures, and gaps in network segmentation, to gain access to the personal information of millions of consumers, including passport information, payment card numbers, Starwood loyalty numbers, name, gender, date of birth, address, email address, telephone number, username, and hotel stay and other travel information. Such prolonged exposure of the highly detailed and individualized personal information in the records contained on Starwood's network has caused or is likely to cause substantial injury to consumers.

29. For example, in the Third Breach, the theft of loyalty account numbers enabled malicious actors to fraudulently make purchases by redeeming loyalty points. In addition, identity thieves are likely to use loyalty account information to gain access to consumers' loyalty accounts and modify login information so that they can redeem points in the future or transfer the loyalty points to another loyalty account controlled by the identity thief. Compared to payment cards, loyalty accounts are more susceptible to fraud due to the value of the loyalty account points, the static nature of account numbers, and the lack of routine monitoring by consumers. As a result, likely because obtaining access to loyalty accounts and redeeming loyalty points is easier than obtaining and using stolen payment card numbers, malicious actors are known to pay more for loyalty account information on the dark web than payment card information. And, in contrast to payment cards, consumers do not have the same legally protected recovery rights when identity thieves fraudulently redeem loyalty points.

30. Similarly, the exposure of more than 5.25 million unencrypted passport numbers in the Second Breach, when combined with the other types of personal information contained in the exposed 339 million records, has caused or is likely to cause substantial injury to consumers. Malicious actors can combine stolen passport information, along with other personally identifying information in the records of Starwood, to create highly successful, targeted phishing campaigns to commit identity theft or other types of financial fraud. Such information is highly valuable on the open market, and wrongdoers frequently seek to purchase passport numbers on the dark web.

31. Consumers have also suffered, and will continue to suffer, additional injuries due to the significant amount of highly detailed and individualized personal information exposed. These injuries include wasted time and money to obtain identity theft protection services, detect

and monitor financial and loyalty accounts for identity theft, replace passports, and cancel and replace compromised payment cards.

32. These harms were not reasonably avoidable by consumers, as consumers had no way to know about Respondents' information security failures described in Paragraph 27 above.

## **VIOLATIONS OF THE FTC ACT**

### **Count I – Respondents' Deceptive Security Statements**

33. Through the means described in Paragraphs 24 and 26, Respondents have represented, directly or indirectly, expressly or by implication, that they used appropriate safeguards to protect consumers' personal information.

34. In truth and in fact, as described in Paragraph 27, Respondents did not use appropriate safeguards to protect consumers' personal information. Therefore, the representations set forth in Paragraphs 24 and 26 is false or misleading.

### **Count II – Respondents' Unfair Information Security Practices**

35. As alleged in Paragraphs 27 to 32, Respondents' failure to employ reasonable security measures to protect consumers' personal information caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. This practice was, and is, an unfair act or practice.

### **Violation of Section 5**

36. The acts and practices of Respondents, as alleged in this Complaint, constitute unfair or deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this \_\_\_\_day of \_\_\_\_, 2024, has issued this complaint against Respondents.

By the Commission & R P P QVHL R R O \ R D N U H F X V H G

April J. Tabor  
Secretary

SEAL: